A Novel Protection Scheme for Quality of Service Aware WDM Networks

W. Fawaz, F. Martignon, K. Chen, G. Pujolle

Abstract—

One of the major concerns of optical network operators is related to improving the availability of services provided to their highest-class clients through the use of different protection schemes. However, the majority of the work concerning protection schemes considered the primary connections as equally important when contending for the use of the backup resources. As a first contribution we therefore propose an improvement of the existing shared protection schemes through the introduction of relative priorities among the different primary connections contending for the access to the protection path. Moreover, as a second contribution, we propose to include a novel service differentiation parameter, the *service disruption rate* of a connection, to provide differentiated services in a WDM mesh network, and we motivate the use of such a parameter with numerical examples. As a third contribution, we present a mathematical model for both the classical protection schemes and for the proposed priority-aware scheme. As a key distinguishing feature from existing literature we derive explicit analytic expressions for the average availability and service disruption rate resulting from the deployment of such schemes. By solving these models we then evaluate numerically the benefits of the service differentiation feature introduced in our scheme as well as the impact of the service disruption rate as service differentiator.

***Index Terms*: - Optical Networks, Protection, Mathematical Models, Quality of Service Provisioning.**

I. INTRODUCTION

The revolutionary Wavelength-Division multiplexing (WDM) technology increases the transmission capacity of fiber links by several orders of magnitude. As WDM keeps on evolving, fibers are witnessing a huge increase regarding their carriage capacity, which has already reached the order of terabits per second. Therefore, the failure of a network component (e.g., a fiber link, an optical cross connect, an amplifier, a transceiver, etc) can weigh heavily on optical carrier operators due to the consequent huge loss in data and revenue. To get an estimate of the different optical components failure characteristics, Table I presents the mean failure rates and failure repair times of various optical network components according to Bellcore (now Telecordia) [1], where Failure-In-Time (FIT) denotes the average number of failures in 10^9 hours, Tx denotes optical transmitters, Rx denotes optical receivers, and MTTR stands for Mean Time To Repair.

W. Fawaz and K. Chen are with the University of Paris 13 - L2TI Lab, 99, Avenue Jean-Baptiste Clement, 93430 Villetaneuse, France E-mail: wissam.fawaz@isep.fr, chen@galilee.univ-paris13.fr

F. Martignon is with the Dipartimento di Ingegneria Gestionale e dell'Informazione, University of Bergamo, Dalmine (BG) 24044, Italy. E-mail: martignon@elet.polimi.it

G.Pujolle is with the University of Paris 6, LIP6 Laboratory, 8 rue du Capitaine Scott, 75015, Paris, France E-mail: guy.pujolle@lip6.fr

Metric	Telecordia Statistics
Equipment MTTR	2h
Cable-cut MTTR	12h
Cable-cut rate	501142 FIT/1000 sheat miles
Tx failure rate	10867 FIT
Rx failure rate	4311 FIT

TABLE I
FAILURE RATES AND REPAIR TIMES (TELECORDIA [1])

Two main conclusions may be drawn based on these statistics: the frequency of failure occurrence in optical networks is not negligible; moreover, cable cut is the dominant failure scenario, compared to Tx and Rx failures, for lengths in the order of hundreds of kilometers, normally found in backbone optical networks. With the frequent occurrence of fiber cuts and the tremendous loss that a failure may cause, network survivability, together with its impact on network design, becomes a critical concern for operators who strive to keep up with the competition for broadband traffic transport. Moreover, as WDM networks migrate from ring to mesh topology, planning a survivable WDM mesh network has been the subject of extensive studies [2], [3], [4] leading to the definition of various resilience approaches. Mainly, there are two types of fault recovery mechanisms: *protection* [5] and *restoration* schemes [6]. In this paper we focus our study on protection schemes, dealing mainly with the impact these schemes have on the customer-perceived service quality which is an emerging topic and of special interest today. We believe that protection, a proactive procedure, is a key strategy to ensure fiber network survivability.

To the best of our knowledge what still lacks in existing literature is a systematic methodology to efficiently select a cost-effective protection scheme for each connection, while satisfying its quality of service (QoS) requirements. Usually, by means of service contracts called Service Level Agreements (SLA), a client subscribes to optical network services from the optical operator with a certain guaranteed QoS level. Within the SLA, Service Level Specifications (SLS) [7] quantify the quality of service provided to the customer. A certain number of SLSs indicate the reliability constraints needed by the subscribed service. Reliability parameters presented in the literature include mainly service availability, and restoration time. Our interest will be directed to service availability since the problem of how connection availability is affected by network failures is currently attracting more research interest.

Contributing to the design of new quality of service aware protection schemes, we propose an extension for the so-called shared protection scheme. To date, the majority of the work

concerning shared protection considered the primary connections as equally important when contending for the use of the backup resources. From a service perspective, this scheme does not provide an optimal solution as it does not take into account the different QoS requirements of the primary connections during the recovery procedure. To cope with such limitation, we envision through our proposal to introduce a relative priority among the primary connections sharing backup resources.

Furthermore, as a second contribution of this paper, we propose the use of a novel QoS metric, the *service disruption rate*, besides service availability, in order to provide differentiated services in a WDM mesh network. In fact, two connections may have the same availability during their entire service periods; however, one of them may experience fewer network failures with longer service downtime for each failure, while the other may experience more network failures with shorter service downtime. Although the two connections have the same service availability, they experience different service disruption rates, which may lead to different customer-perceived service qualities.

In order to gauge the benefits of our proposals, we evaluate numerically both the service differentiation feature introduced in the proposed priority-aware scheme as well as the impact of the service disruption rate as a service differentiator. Therefore, we present a mathematical model for both the classical shared-protection schemes and the proposed priority-aware scheme. Then by solving these models, we derive explicit analytic expressions for the average availability and service disruption rate resulting from the deployment of such schemes.

The paper is structured as follows: in Section II we propose and describe the priority-aware shared protection scheme; in Section III we introduce a mathematical model to evaluate the impact of the protection schemes analyzed in this paper on the proposed Quality of Service parameters (availability and service disruption rate); in Section IV we present numerical results to evaluate the benefits of the service differentiation feature introduced in our scheme as well as the impact of the service disruption rate as service differentiator. Finally, Section V concludes this paper and proposes future issues.

II. Priority-Aware Shared-Protection Scheme

This Section introduces our novel scheme that extends the existing shared-protection schemes through the introduction of relative priorities among different primary connections contending for the backup paths. Let us consider N working paths $(w_i, i = 1, \ldots, N)$ with the same source and destination sharing M backup paths $(b_i, i = 1, \ldots, M)$, i.e. an M:N protections scheme, as depicted in Figure 1. Both work paths and backup paths can be in failure. When a failure occurs, the repair process is started.

In the classical shared-protection scheme, when several subsequent failures happen in the network, all connections are considered of equal importance when contending for backup resources. As such, the first failed connection gains access to the backup path.

On the other hand, in our proposed scheme these connections are divided into K sets of reliability classes, $C_1, \ldots, C_K$, with N_i connections belonging to class C_i for $i = 1$ to K, and $\sum_{i=1}^{K} N_i = N$. Connections belonging to class C_1 have the highest priority, while those belonging to C_K have the lowest priority. When the working path of a connection t belonging to class C_i breaks down, the first available backup path, if any, is assigned to protect connection t and restoration is ensured by switching t to the backup path. Meanwhile, repair actions are performed on the primary path to restore it to be as good as new. Once repairing the primary path is achieved, the restored connection is switched back to its primary path. On the contrary, if at the moment t fails all the backup paths are already occupied protecting other connections, a check is made to verify the existence of protected connections belonging to classes of lower priority than t, i.e. to classes comprised between $i + 1$ and K. If several such connections exist, the one having the lowest priority is immediately preempted by connection t. The preempted connection thus becomes unavailable, waiting for a backup path to be freed or for its working path to be repaired. Finally, if neither of the two above situations is verified, connection t becomes unavailable.

III. The Mathematical Model

In this Section, we present a mathematical model for both the classical 1:N shared protection scheme and the corresponding priority-aware extension discussed previously. Solving this model, we derive explicit expressions for the average availability and service disruption rate of a connection resulting from deploying the aforementioned protection strategies. It is important to note that the dedicated protection case can be viewed as a special case of the shared protection scheme with N=1.

We are interested in the following metrics: *availability* and *service disruption rate* of a connection. The availability of a connection is defined as the probability that such connection is "up" at any given time [8], and can be expressed as the proportion of time the connection is up during its entire service. If a connection is carried by a single unprotected path, its availability is equal to the path availability. The service disruption rate of a connection is defined as the average number of transitions from an available to an unavailable state per one time unit.

The availability of a protected connection is determined by both the primary and the backup paths. In other words, a protected connection t is said to be *available* when either no failure affects its primary path or it is recovered by the backup path in case of failure along the primary path. Connection t becomes *unavailable* in the following two cases:

- one failure occurs on the primary path of t and a second failure occurs on its backup path;

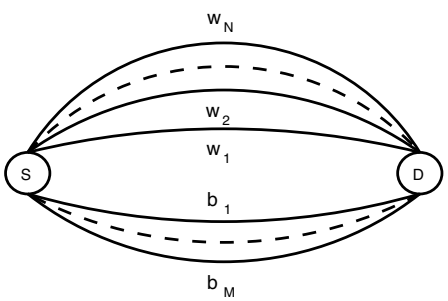

Fig. 1. N working paths sharing M backup paths between a source node S and a destination node D.

- if t shares the backup path with connection t', then t will be unavailable if both t and t' fail but the shared backup path is taken by t'. In the priority-aware scheme, this happens if t' has higher priority than t.

In this study we disregard the impact of the reconfiguration time for switching traffic from primary paths to backup paths on availability, since this time is negligible (usually on the order of milliseconds) compared to the failure repair time (usually on the order of hours) and to the connection's holding time (usually in the order of weeks or months).

A. Basic Assumptions

We base our mathematical study on the following classical assumptions [9]:

- a connection has only two states: it is either available or unavailable.
- Different network components fail independently leading to repair actions.
- Sufficient resources are available to repair simultaneously any number of failed connections, restoring them to be as good as new. This is known in the literature as *unlimited repair* [9].
- For any component the inter-failure time and the repair time are independent stationary Markovian processes with known mean values: Mean Time To Failure (MTTF) and Mean Time To Repair (MTTR), respectively.

A path holding a connection t fails when at least one of the components along the path is defective. The contribution of cable-cut rate to the overall path failure rate is predominant, compared to that of other components. Hence, for the sake of simplicity we assume that the failure rate λ of a path is equivalent to that of a single cable-link having the same length as the considered path. As a result, to compute the failure rate of each path we can multiply its length to the cable cut-rate per length unit (see Table I).

B. Model Definition and Resolution for the Classic Shared-Protection Scheme

Let us consider N working paths that share the same backup path, i.e. a 1:N shared-protection scheme. Let $\lambda_i, i = 1, ..., N+1$ be the mean failure rate of the *i-th* path and μ_i be the mean recovery rate of the *i-th* path; $\frac{1}{\lambda_i}$ and $\frac{1}{\mu_i}$ hence represent the Mean Time To Failure and Mean Time To Repair of the *i-th* path, respectively. Based on the above assumptions, all the path failures are statistically independent, and interfailure and repair times are exponentially distributed.

To gain insight into the behavior of the system and according to existing literature [10], [9], we will consider a case of special interest in which all the paths (working as well as backup ones) have identical failure and recovery rates, i.e. $\lambda_i = \lambda$ and $\mu_i = \mu, \forall i = 1, \ldots, N+1$. Let us define $\rho = \frac{\lambda}{\mu}$. We have here a classical problem of reliability, with 1 redundant unit for N working units. Here a unit is an optical path.

The steady-state availability A_i of a single path i, viz. the limiting ($\tau \to \infty$) probability of finding the path successfully operating at time t, can be calculated as follows:

$$A_i = \frac{MTTF}{MTTF + MTTR} = \frac{1/\lambda}{1/\lambda + 1/\mu} = \frac{1}{1+\rho} \quad (1)$$

$\overline{A_i} = 1 - A_i$ represents the unavailability of path i.

Let $F(\tau)$ be the number of failed paths at time t. Because of the assumptions, $F(\tau); \tau \geq 0$ forms a continuous and stationary Markov process, with $F(0) = 0$. Let $p(n)$ be the steady state probability that $F(\tau) = n$ in stationary regime. The transition diagram is given in Fig. 2.

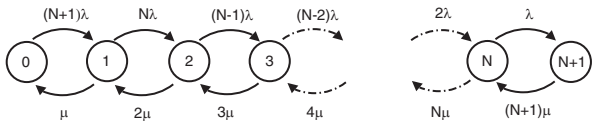

Fig. 2. Transition Diagram

After some classical calculus we can express the steady state probability $p(n)$ of the Markov chain as follows [11], [9]:

$$\begin{aligned} p(n) &= C_{N+1}^{n} \overline{A}^{n} A^{N+1-n} \\ &= \frac{(N+1)!}{n!(N+1-n)!} \frac{\rho^n}{(1+\rho)^{N+1}} \end{aligned} \quad (2)$$

where C_{N+1}^{n} represents the number of all combinations of n failed paths out of $N+1$, and A is given by equation (1). In other words, the number of failed paths follows a binomial distribution with parameters $N+1$ and $\overline{A}$.

Note that $p(n)$ represents the proportion of time in which there are n failures in the network. When the total number of path failures n is greater than or equal to one, we can distinguish two cases:

1) the backup path is among the failed paths and the remaining $n-1$ connections cannot be restored;
2) all the n failed paths are primary paths, and as such, only one connection is restored by the backup path while the remaining $n-1$ are not.

Therefore, under such conditions there will always be exactly $n-1$ unavailable connections. For $n \geq 2$ at least one connection will be unavailable, while when the number of failures n is equal to 1, there will be no unavailable connections.

From this classical result, we are now interested in calculating the average unavailability and the average service disruption rate of a specific connection t among the N shared-protected ones. The average unavailability of t is the proportion of time such connection is unavailable for all possible numbers of failures n, $2 \leq n \leq N+1$.

Let us define $Y(n)$ the event of t being unavailable under state n.

The probability of having our reference connection t unavailable when there are n failed paths is equal to $p(n)P(Y(n))$. As $p(n)$ has already been calculated in equation (2), what remains is to calculate $P(Y(n))$. To do so, we have to consider all the events that may lead to the connection t becoming unavailable under state n. These events are the following:

- $W(n)$: both the primary path of connection t and the backup path are failed;
- $Z(n)$: connection t's primary path is failed but the backup path is available.

Building on this information and according to the theorem of total probability, $P(Y(n))$ can be calculated as follows

$$P(Y(n)) = P(Y(n)|W(n))P(W(n)) + + P(Y(n)|Z(n))P(Z(n)) \quad (3)$$

where $P(Y(n)|W(n))$ and $P(Y(n)|Z(n))$ are, respectively, the conditional probabilities of having our reference connection t unavailable, given that events $W(n)$ and $Z(n)$ occurred. $P(Y(n)|W(n)) = 1$ as the backup path in this case is failed and no restoration is possible; $P(Y(n)|Z(n)) = \frac{n-1}{n}$ as only one of the n primary paths under failure in this case can be restored.

The probability of the event $W(n)$ is:

$$P(W(n)) = \frac{C_{N-1}^{n-2}}{C_{N+1}^{n}} = \frac{n(n-1)}{N(N+1)} \quad (4)$$

where the numerator indicates all possible combinations where the primary path of connection t and the backup path are among the failures. The denominator indicates all possible combinations of n failed paths out of $N+1$.

The probability of the event $Z(n)$ is:

$$P(Z(n)) = \frac{C_{N-1}^{n-1}}{C_{N+1}^{n}} = \frac{n(N+1-n)}{N(N+1)} \quad (5)$$

where the numerator indicates all possible combinations where the primary path of the connection t is among the failures while the backup is not.

Then, based on the above equations, the probability P(Y(n)) that the observed connection t is unavailable under state n is equal to:

$$P(Y(n)) = \frac{n-1}{N},\ 2 \leq n \leq N+1 \quad (6)$$

It can be seen that this equation is also valid for the case $n = 1$, for which $P(Y(n)) = 0$, since in this case all connections will be available, as stated before.

Based on the theorem of total probability, the unavailability of a connection in the case of 1:N protection is given by the following formula:

$$U(N,\lambda,\mu) = \sum_{n=2}^{N+1} p(n) \cdot P(Y(n)) = \sum_{n=2}^{N+1} p(n) \cdot \frac{n-1}{N} \quad (7)$$

and, substituting the expression (1) for $p(n)$ we obtain:

$$U(N,\lambda,\mu) = \frac{1}{N} \cdot \sum_{n=2}^{N+1} \frac{(n-1) \cdot C_{N+1}^{n} \cdot \rho^n}{(1+\rho)^{N+1}} \quad (8)$$

The average availability for a connection is simply equal to $1 - U(N,\lambda,\mu)$.

Following the guidelines given in [12], let us now calculate the average service disruption rate of a given connection t. According to equation (6) the probability that a given path is unavailable in state n, with $n \geq 1$, is equal to $\frac{n-1}{N}$. Hence, the probability that such connection is available is equal to $1 - \frac{n-1}{N}$.

This probability corresponds to two distinct events, i.e.

- connection t is up;
- connection t's primary path is failed but t is restored by the backup path.

In the first case, as $n \geq 1$, we are sure that the backup path is either occupied to restore one of the n failed connections or it is among such failures. Hence, when connection t breaks down, it has no possibility of restoration by the backup path and it transits from an available to an unavailable state at a rate equal to the failure rate of its working path, λ.

In the second case, such transition happens when the backup path fails, again at rate equal to λ.

The expression of the average service disruption rate, $S(N,\lambda,\mu)$ is thus the following:

$$S(N,\lambda,\mu) = \lambda \sum_{n=1}^{N+1} (1 - \frac{n-1}{N}) \cdot p(n) \quad (9)$$

and, substituting the expression of $p(n)$ we obtain the following expression:

$$S(N,\lambda,\mu) = \frac{\lambda}{N} \cdot \sum_{n=1}^{N} \frac{(N+1-n) \cdot C_{N+1}^{n} \cdot \rho^n}{(1+\rho)^{N+1}} \quad (10)$$

C. Model Definition and Resolution for the Priority-Aware Scheme

Let us consider the priority-aware shared-protection system proposed in Section III, where N connections are divided into two sets of reliability classes, C_1 and C_2, with N_1 and N_2 connections belonging to class C_1 and C_2, respectively, and $N_1 + N_2 = N$. Connections of class C_1 have higher priority than connections belonging to C_2.

In the following we derive the analytic expressions for the availability and the service disruption rate for each connection according to its priority class.

We will begin by considering higher-priority connections. First of all, the N_1 connections having the highest priority can preempt instantaneously all the other connections belonging to the lower-priority class in the utilization of the backup path. Consequently, the analysis of the proposed scheme with regard to the high-priority connections is equivalent to the study of a classic 1:N_1 shared-protection scheme.

Therefore, we can derive straightforwardly the average unavailability U_1 and service disruption rate S_1 of high-priority class connections based on equations (8) and (10) by simply substituting N with N_1.

When a low-priority connection fails, it becomes unavailable if any of the following mutually exclusive conditions is verified:

1) the protection path has already failed;
2) the protection path is up but there is at least one high-priority connection among the failures;
3) the protection path is up, no high-priority connections are among failures, there is however another low-priority connection occupying the protection path.

Let E_i be the event of having condition i verified, $i = 1, 2, 3$. Therefore, to study the unavailability U_2 of a low-priority connection, we consider the process $Q(\tau)$ whose general state is a

triplet (n_1, n_2, b), where n_1 and n_2 indicate, respectively, the number of failed high and low-priority connections at time τ, and b is a flag set to 1 if the backup path is down and to 0 if it is up.

$Q(\tau)$ is a continuous and stationary Markov process, with a limiting probability for each state given by

$$P(n_1, n_2, b) = P(n_1)P(n_2)P(b) \tag{11}$$

where $P(n_1)$, the probability of having n_1 failed high-priority connections and $P(n_2)$, the probability of having n_2 failed low-priority connections, are respectively equal to:

$$P(n_1) = C_{N_1}^{n_1} \overline{A}^{n_1} A^{N_1 - n_1} \tag{12}$$

$$P(n_2) = C_{N_2}^{n_2} \overline{A}^{n_2} A^{N_2 - n_2} \tag{13}$$

and A is given by equation (1). $P(b)$ is the probability of having b backup path failures. In other words, when $b = 0$, there is no failure affecting the backup path, whereas if $b = 1$ the backup path is down. The expression of $P(b)$ is:

$$P(b) = \overline{A}^b A^{1-b} \tag{14}$$

The events $(E_i, i = 1, 2, 3)$, leading to the unavailability of a low-priority connection, are verified according to the values of n_1, n_2 and b. So, $b = 1$ leads to E_1, meaning that the protection path has failed; on the other hand, $b = 0$ and $n_1 \geq 1$ lead to event E_2; finally, $b = 0$, $n_1 = 0$ and $n_2 \geq 2$ produce event E_3.

Under state (n_1, n_2, b), a specific low-priority connection t is unavailable when it fails *and* one of the events $E_1 - E_3$ is produced. Based on this observation, U_2 is given by:

$$\begin{aligned} U_2 &= \sum_{\forall (n_1, n_2, b)} P(t \text{ fails in state } (n_1, n_2, b)) \times \\ &\times \; P(n_1, n_2, b) \times P(E_1 \cup E_2 \cup E_3) \end{aligned} \tag{15}$$

where:

$$P(t \text{ fails in state } (n_1, n_2, b)) = \frac{C_{N_2-1}^{n_2-1}}{C_{N_2}^{n_2}} \tag{16}$$

and $P(E_1 \cup E_2 \cup E_3)$ can be obtained with classical manipulations. It follows that U_2 is equal to:

$$\begin{aligned} U_2 &= \sum_{i=2}^{N_2+1} C_{N_2-1}^{i-2} \overline{A}^i A^{N_2-i+1} + \\ &+ \sum_{i=1}^{N_2} C_{N_2-1}^{i-1} \overline{A}^i A^{N_2-i+1} \cdot (1 - A^{N_1}) + \\ &+ \sum_{i=2}^{N_2} C_{N_2-1}^{i-1} \overline{A}^i A^{N_2-i+1} \cdot A^{N_1} \cdot \frac{(i-1)}{i} \end{aligned} \tag{17}$$

We note that equation (17) can be also obtained with the following reasoning based on the conservation law presented in [13] adapted to our study case.

In fact, the classical shared-protection scheme and the priority-aware extension under study can be viewed as two different scheduling schemes for organizing the access to a shared resource which is the backup path. Therefore, an invariant relation of the following form is obtained:

$$\sum_{i=1}^{N} \rho_i W_i = C \tag{18}$$

where in our case ρ_i is equivalent to the already defined ρ, W_i is the average unavailability of connection i, and C is a constant.

Note that $W_i = U_1$ if connection $i \in C_1$ and $W_i = U_2$ if $i \in C_2$.

Considering the same number of primary paths N in the two schemes, equation (18) becomes

$$U(N, \lambda, \mu) \cdot N = U_1 \cdot N_1 + U_2 \cdot N_2 = C \tag{19}$$

As such, U_2 is equal to

$$U_2 = U(N, \lambda, \mu) \cdot \frac{N}{N_2} - U_1 \cdot \frac{N_1}{N_2} \tag{20}$$

Following the same reasoning, we can compute the service disruption rate S_2 of a low-priority connection as follows:

$$S_2 = S(N, \lambda, \mu) \cdot \frac{N}{N_2} - S_1 \cdot \frac{N_1}{N_2} \tag{21}$$

IV. Numerical Results

In this Section we gauge the benefits of the service differentiation feature introduced through the proposed priority-aware protection scheme, then we evaluate the impact of the service disruption rate as a service differentiator. For the sake of simplicity, we consider a scenario consisting of 3 primary connections sharing one backup path. We first consider a priority-aware protection scheme, with one high-priority and two low-priority primary connections. The availability of each class is calculated for different connections' lengths based on equations (19) and (20), and is reported in Figure 3. Then, a classical shared protection scheme is applied to this scenario, and the availability of a connection is evaluated using equation (8). The corresponding results are reported again in Figure 3 for comparison purposes. It is important to state that the Mean Time To Repair ($\frac{1}{\mu}$) of all the paths is considered equal to 12 hours (see Table I).

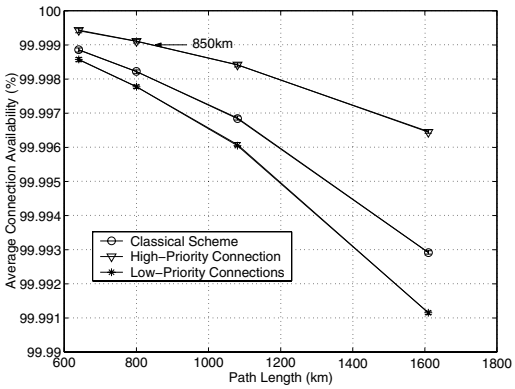

Fig. 3. Average availability for the classical and the priority-aware 1:3 shared-protection scheme

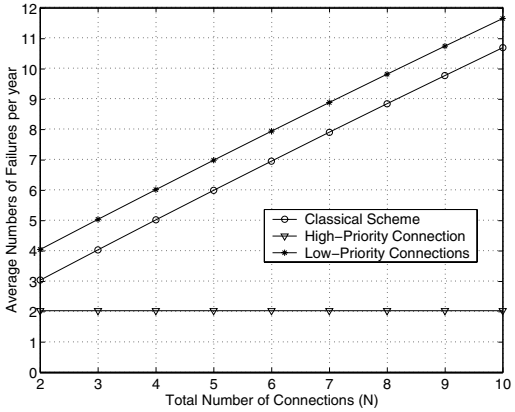

Fig. 4. Average number of failures per year for the classical and the priority-aware 1:N shared-protection scheme, with 1 high-priority connection and N-1 low-priority ones

Based on Figure 3 we can observe that the high-priority connection protected using the priority-aware scheme is more available than the connections protected by the classical shared scheme.

The observed availability results can be interpreted from a Quality of Service level perspective using the following reasoning. According to [7] a Gold client requests an availability of 99.999% (i.e. at most 5 minutes of unavailability per year), whereas a Silver client requires an availability of 99.99% per year. With regard to this QoS terminology, the high and the low-priority classes can be mapped into Gold and Silver QoS levels [7] or to lower QoS classes according to the connection's length. In fact, as shown in Figure 3, the availability of the high-priority connection drops below 99.999% when the connection length exceeds 850km, while in the classical scheme this target availability is never achieved. This proves that by deploying the proposed scheme, Gold connections provisioning becomes possible in the network even for long communications which are encountered typically in backbone optical networks. Moreover, the QoS level of the Silver connections is still maintained.

To backup the mathematical analysis we also simulated the previously discussed scenario using a discrete-event simulation tool [14], and the results are again shown in Figure 3. Each availability value has been calculated over multiple simulations to achieve very narrow 97.5% confidence intervals. We note that simulation results practically overlap analytic data in every situation, thus backing-up the analytic approach.

Finally, we evaluate the impact of service disruption rate as a service differentiator. We still consider the same scenario with 3 primary connections and one backup path presented above. For illustration purposes, we consider a reference connection cut-rate $\lambda = 1/250\, h^{-1}$. The service disruption rate experienced in a reference period of one year for the classical 1:3 scheme, calculated based on equation (10), is approximately equivalent to 6 service disruptions per year. For the priority-aware scheme, the high-priority connection experiences in average 3 service disruptions per year while the low-priority ones become unavailable in average 7 times per year. Hence, the rate at which the high-priority connection becomes unavailable is approximately the half of that experienced by classically protected connections. In the following study, the number N of primary connections is varied between 2 and 10, to gain insight into the impact of such variation on the service disruption rate. First, a priority-aware scheme is assumed with only 1 connection of high-priority. Then the classical 1:N protection scheme is applied. In Figure 4, the service disruption rates for the different primary connections are depicted. These results demonstrate the advantage of the priority-aware approach as the gain realized is consistent.

V. Conclusions and Future Issues

In this paper we proposed an improvement of the existing shared protection schemes through the introduction of relative priorities among the different primary connections contending for the access to the protection path. We introduced a novel service differentiation parameter, the *service disruption rate* of a connection, to provide differentiated service in a WDM mesh network, and we motivated the use of such parameter with numerical examples. Finally, we presented a detailed mathematical model for both the classical shared-protection schemes and for the proposed priority-aware scheme. We derived explicit analytic expressions for the average availability and service disruption rate resulting from the deployment of such schemes.

The introduction of the priority-aware protection scheme, of the service disruption rate, and of the models studied in this paper have a generic fundamental significance, beyond the specific context of path protection in WDM networks. Indeed, they can be applied to general systems. Due to this generality, any further results that can be derived have a potential significance for other fields.

References

[1] Jing Zhang and S.Mukherise. A review of fault management in WDM mesh networks: basic concepts and research challenges. In *IEEE Network*, pages 41–48 vol.18(2), March-April 2004.

[2] S.Ramamurthy, L.Sahasrabuddhe, and B.Mukherjee. Survivable WDM mesh networks. In *Journal of Lightwave Technology*, pages 870–883, vol. 21(4), April 2003.

[3] G.Mohan, S.R.Murthy, and A.K.Somani. Efficient Algorithms for Routing Dependable Connections in WDM Optical Networks. In *IEEE/ACM Transactions on Networking*, pages 553–566 vol.9, Oct. 2001.

[4] G.Ellinas, A.Hailemariam, and T.E.Stern. Protection Cycles in Mesh WDM Networks. In *IEEE Journal on Selected Areas in Communications*, pages 1924–1937 vol.18, October 2001.

[5] S.Ramamurthy and B.Mukherjee. Survivable WDM Mesh Networks, Part I – Protection. In *Proceedings of INFOCOM'99*, pages 744–751, March 1999.

[6] S.Ramamurthy and B.Mukherjee. Survivable WDM Mesh Networks, Part II – Restoration. In *Proceedings of IEEE International Conference on Communications (ICC '99)*, pages 2023–2030, June 1999.

[7] W.Fawaz, B.Daheb, O.Audouin, B.Berde, M.Vigoureux, M.Du-Pond, and G.Pujolle. Service Level Agreement and Provisioning in Optical Networks. In *IEEE Communications Magazine*, June 2004.

[8] M.To and P.Neusy. Unavailability Analysis of Long-Haul Networks. In *IEEE Journal on Selected Areas in Communications*, pages 100–109 vol.12(1), 1994.

[9] J.E.Angus. On computing mtbf for a k-out-of-n:g repairable system. In *IEEE Transactions on Reliability*, volume Vol 37(3), pages 312–313, August 1988.

[10] D.Lee, L.Libman, and A.Orda. Path Protection and Blocking Probability Minimization in Optical Networks. In *Proceedings of INFOCOM'04*, 7-11 March 2004.

[11] D.Mitra. Stochastic Theory of a Fluid Model of Producers and Consumers Coupled by a Buffer. In *Advances in Applied Probability*, pages 646–676 vol.20, 1988.

[12] A.Birolini. *Quality and Reliability of Technical Systems: Theory, Practice, Management*. Springer-Verlag, Berlin, 1997.

[13] L.Kleinrock. *Queueing Systems, volume 2*. John Wiley, 1976.

[14] M.Veran and D.Potier. *QNAP 2: A Modeling Language for Mathematical Programming*.